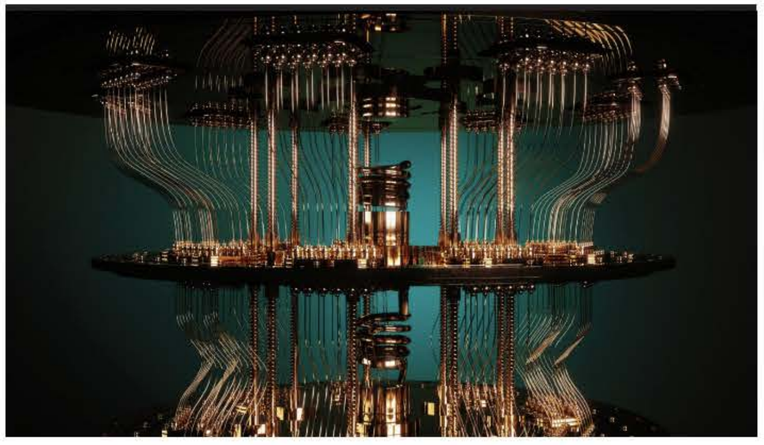
A quantum leap for pensions?

What is quantum computing, how does it work – and could it be poised to revolutionize plan members' retirement?



QUANTUM COMPUTING is an emerging technology with the potential to profoundly affect all industries, including pensions.

In describing quantum computers, it helps to contrast them with current or "classical" computers, which use tiny transistors to generate informational bits with the value of zero or one. To execute a computer program, transistors are continually switched on and off according to logic that encodes the problem being solved. The development of classical computer technology since the middle of the last century has relied on making the transistors smaller and the switching faster. Although progress has proceeded exponentially, leading to the modern information age, the growth is slowing due to hard physical limits on the size and switching speed of transistors.

Quantum computers, by contrast, use the principle of quantum superposition, which has no classical analogue. A quantum bit, called a qubit, isn't constrained by needing to be either off or on. Until we measure it, we need to treat it as if it were in both states simultaneously. Many popularisations of quantum mechanics describe this using Schrodinger's famous analogy of a cat in a box which may or may not have been poisoned. Until we open the box and confirm the cat's fate, it is in a combined state of being both alive and dead. In addition, multiple qubits can be "entangled," meaning that they are intrinsically correlated with one another. The use of superposition and entanglement allows for qualitatively different algorithms that have no analogue in classical computers and that can, in some cases, be dramatically faster. We discuss examples relevant for pensions later on.

There are many ways to create a quantum computer – such as trapped ions, neutral atoms, superconductors, quantum dots, and other novel physical systems. However, it is still very difficult to create a large-scale machine. The current record, set in October of 2023, is only 1,180 qubits, compared to the billions of bits in a typical classical computer. In addition, the superposition of the quantum state is exceedingly fragile, and maintaining the state long enough to perform a useful calculation is a challenge. There has been rapid progress on addressing these engineering issues. In the rest of this article, we shall assume that these developments will continue and allow for practical applications for financial institutions such as pensions.

Cryptography is of central importance to our highly networked world. This is certainly true for pensions where use of cryptography means that members are assured that their personal information is kept private. In addition, portfolio managers must communicate securely with service providers, among dozens of applications. Quantum computers have the potential to break modern encryption.

All encryption algorithms rely on the concept of what is called a trapdoor function. This is an operation that is very easy to perform in one direction, but is effectively impossible to undo. One common example is the multiplication of prime numbers. A prime number is a number that cannot be written as the product of smaller numbers: 61 and 53 are prime numbers. In contrast, a composite number is a product of primes: for example, 3,233 is a composite number, since it equals 61 times 53. The trapdoor is to determine the two prime numbers if all you know is their product. Even in our simple example, most people would find multiplying 61 times 53 to be much simpler than finding the unique factors of 3,233. The difference in difficulty is exponentially greater if the two prime numbers are sufficiently large. Modern cryptography uses numbers that are over 600 digits long, so that even the fastest computer in the world would require billions of years to factor them. This means that you can broadcast the product while remaining confident that no one can infer the two underlying primes, which effectively remain secret.

Quantum computers could crack this problem. One early result in quantum computing was the Shor algorithm, which shows that factoring is tractable for a quantum computer. And recently, another researcher published a refinement that could be up to 1,000 times faster still. This has the potential to upend cryptography. Even though no one is yet close to having a quantum computer that can effectively implement the Shor algorithm, there is the concern that bad actors could archive encrypted data today in the hopes of being able to crack it later, once quantum computers are available. This concern goes by the handle "harvest now, decrypt later," and has injected urgency into research on so-called post-quantum cryptography – the search for cryptographic algorithms that are equally difficult for classical and quantum computers.

Optimization is another important application. In some instances, dramatic speedups have been reported on optimization problems. D-Wave Systems, based in Burnaby, BC, has developed quantum machines that are specific to that application. A third application is to Monte Carlo simulation, an algorithm that uses large numbers of random synthetic scenarios for the system being modelled and then averages the result. Unfortunately, the approach is very slow: to double the accuracy, you need four times the number of scenarios. Quantum computers are different: to double the accuracy you only need double the number of scenarios. Many financial applications require hundreds of millions of scenarios, and quantum computers could provide the same accuracy with orders of magnitude fewer scenarios.

Improvements in decision-making include applications to risk management and finance. Risk management relies heavily on quantitative techniques like Monte Carlo to support functions such as market risk measurement, counterparty credit risk processes, and actuarial analyses, among others. The use of quantum computers could either speed up existing processes or enhance accuracy or scope. As with machine learning, there may well be applications that are not even currently envisaged. And indeed, marrying the concepts of artificial intelligence and quantum computing is an active area of research.

To close, we remark that there are investment opportunities in the field of quantum computing due to the many start-ups in need of capital. As one example, Photonics, based in Vancouver, has raised over $140 million in funding and has recently partnered with Microsoft to scale up its technology. According to Capgemini, annual investments have grown by a factor of 10 in just the last five years. This space is increasingly attractive for venture capital firms, given the greenfield nature of the industry, the potential for large upside gains, and the diversification provided. BPM

Potential applications for saving money include better automation around due diligence, back-office functions like accounting and trade confirmations, audit functions and anomaly detection

More specific to pensions, quantum computers can help to:

- make money
- save money
- improve the decision-making process

In terms of making money, potential applications include portfolio optimisation, better market forecasting, improved macroeconomic forecasting, and enhanced algorithmic trading. Due to physical constraints on existing quantum computers, optimisation algorithms have so far only been used on unrealistically small portfolios. Nonetheless, they are important proofs-of-concept that show that when the hardware is further developed, the process of portfolio optimisation is primed for disruption.

Potential applications for saving money include better automation around due diligence, back-office functions like accounting and trade confirmations, audit functions, and anomaly detection. Enhanced Monte Carlo could also benefit functions such as derivative valuations.

Davide Sabatini, Niall Whelan, and Ranjan Bhaduri represent the Bodhi Research Group.